ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Implementation of Image Steganography Using FPGA

Deepa. S [*1], Sarankumar. S [2]

[*1] Assistant professor, Karpagam College of Engineering, Coimbatore, India

[2] Service Engineer, Texmo Industries, Coimbatore, India

deepaa.selva@gmail.com

Abstract

Steganography is the art and science of communicating in a way which hides the existence of the communication. Unlike Cryptography, where the attacker is allowed to detect, intercept, modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganographic method is that no one will be able to know whether anything is hidden in the image or not. For hiding secret message in images, there exists a large variety of steganographic techniques. Few of them are more complex than others and all of them have respective merits and demerits. The requirements of steganographic techniques used, differ in accordance with different applications. Based on the PSNR value of each image, the PSNR value of stego image is higher. The proposed algorithm is the combination of random pixel manipulation methods and Least Significant (LSB) matching of Steganography embedding and extracting method.

Keywords: Steganography, Stego image, LSB algorithm.

Introduction

Image steganography is about hiding the message inside a message without any visible modifications to the real world. Digital image is the most common type of carrier used for steganography. A digital image is composed of finite number of elements each of which has a particular location and value (gray scale). The processing of these digital images by means of a digital Computer is referred as digital image processing. Images are used for Steganography in following ways. The message in encrypted form or in the original form is embedded as the secret message to be sent into a graphic file. As a result of this, stego-image image is produced.

In addition to this, a secret data such as stego key may be needed in the hiding process. The stego-image is transmitted to the receiver. The message is extracted from the carrier image by the receiver. The message extraction is possible only if both the sender and the receiver share the same secret key or any secret parameter. An attacker or stego analyst may try to hack the stego-image.

Digital stenography allows changes to be made to digital carriers like sounds or images. The information has nothing to do with the carrier sound or image. Enhanced Data Hiding Capacity Using LSB Based Image Steganography Method: Images are more popular cover objects because large redundant bits present in the digital image representation. A digital can be represented as 2D matrix. Bit depth of a RGB image is 24.

Spatial and Transform domain are the two techniques to conceal information inside a cover image. This paper approached spatial domain technique. In spatial domain, the secret bits are written directly to the cover image pixel bytes. It uses Least Significant Bit algorithm in which the secret bits are embedded in the last bit of each component of an image. Advantage of this system is easy to implement.

Secret message can be easily identified due to the absence of key and the system doesn't support for larger secret bits are notified as drawbacks. Mean square error, Bit error rate and PSNR are the metrics used to measure the imperceptibility of Steganography.[1] Steganography Algorithm for Hiding data in Image by Improved LSB substitution. By minimize Detection: This paper proposed a new idea that "Visual perception of intensity blue objects is less distinct that the perception of objects of red and green". Hence to embed the message bits, blue channel is used. This system comprising two phases embedding and extracting phase.

In Embedded phase, Extract all the pixels of an image and store it in pixel array. Extract all the characters in the text file and store it in character array and also extract all the characters of stego key and store it in key array. Choose first pixel and pick

ISSN: 2277-9655
Impact Factor: 1.852

character from key array and place it in blue component finally terminate with zero to indicate end of key. Then place message bits in blue channel of all pixels and terminate with zero to indicate end of message.

In extraction phase, extract all the pixels of stego image and store it in pixel array. Scan the first pixel and extract key character from blue component of pixel and place it in key array. If the extracted key matches with the key entered by the receiver then proceed with next pixel else display the message "Key is not matching". The secret message was extracted and put it into character array. LSB algorithm limits the size of the secret bits is the major drawback of the system. [2]FPGA

Implementation of Secured Steganography

Communication System: Color space conversion will lead to hold the quality of an image. The Stego image is represented in RGB color space which is converted to YCbCr color space. Y component gives the brightness information of the color. Cb and Cr provide the hue and saturation information of color which is less sensitive to track by eyes. So the secret bits are embedded in these layers. Pseudo random number generator is used to select some pixels of the cover image. Then the secret will be hidden randomly in the channel of selected pixels. It consists of six different PRNG are used for each channel to set the pixel locations in the three layers. Xtreme DSP kit consists of nallatech ben-one main board, a nallatech –ADDA daughter card and is fitted with a Xilinx virtex-II XC2VP30 FPGA chip. It supports MATLAB/simulink based logic synthesis (HDL).[3]

Steganography for text messages using image in this Steganography system, we embed text data in an image in frequency domain using steganographic algorithm because Steganography in the spatial domain is less resilient to common image processing operations. Hiding information may require a stego key which is additional select information, such as password required for embedding the information.

Table 1: Comparison of the existing systems

S.NO	SYSTEM	MAIN THEME	DISADVANTAGE
1.	Enhanced Data Hiding Capacity Using LSB Based Image Steganography Method (2013)	LSB approach in spatial domain	No secret key
2.	A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection(2012)	Use blue component to embed the stego key	Limits the size of message bits
3.	An FPGA Implementation of Secured Steganography Communication System (2012)	Pseudo random generator for select pixels in the cover image	No Secret Key
4.	Steganography for Text Messages Using Image (2012)	LSB approach in frequency domain	System complexity

In the embedding phase, cover image is dividing into 8X8 block and apply DCT over it. After getting the AC and DC coefficient quantize it. Skip the zero and DC coefficients and embed the message bits using LSB algorithm.

In extraction phase, accept the shared secret password from stego image.[4] By using proposed encoder to decode the coefficient. From the DCT coefficients we can extract the embedded message bit. Some the techniques used and insertion of bits in the lowest bits of noisy images.

Proposed System

In both the Encryption and decryption side same algorithm was proposed so that it was able to retrieve the original message. Here encryption involves the conversion of the data into a stream of byzantine characters .With the evolution of high computing systems it was easily able to crack that kind of algorithms. So to overcome this kind of problems a method known as "Steganography" was introduced. By using this method the message secrecy was ensured, the data was secure during transmission. It was also offered with improved security, robustness and very high data capacity. All these features made Steganography a best way for secure transmission of the data.

Related works

Our proposed method aims to increase the number of bits embedded in each pixel to four, by altering one bit or maximum of two bits in the cover pixel. Compared to the above method this slightly decreases imperceptibility but increases the embedding capacity. And it also maintains the PSNR value in a acceptable range.

ISSN: 2277-9655
Impact Factor: 1.852

In our proposed system first we get an image which has all the basic RGB intensity in an image then we convert it to grey scale so that it is easy perform BITAND operations for encoding the message. Then the grey scale image is allowed to undergo discrete wavelet transforms which separates it to four different intensity LL, LH, HL, HH. Here LL refers to 00 by performing AND operation the output we get 0. Here we can only store the message in the output having 0.So message can be stored in LL, LH and HL only. But we mainly prefer message to be stored in LL so that visibility of the image should be clear then .Then we get a message to embedded in the so formed stego image or transformed image. Then in the embedding phase we store we store the message bits in the rows of the pixel value of the image by shifting the columns and the same reverse algorithm is followed at the decoder side to retrieve the original message from the transformed image.

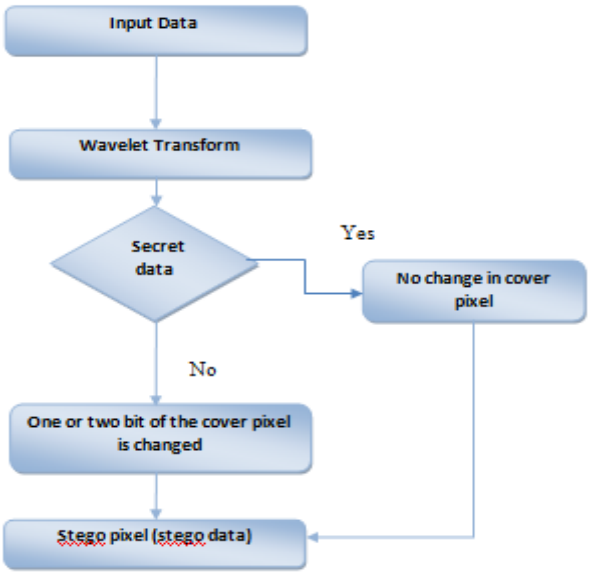

Fig.1. Embedding Flow chart

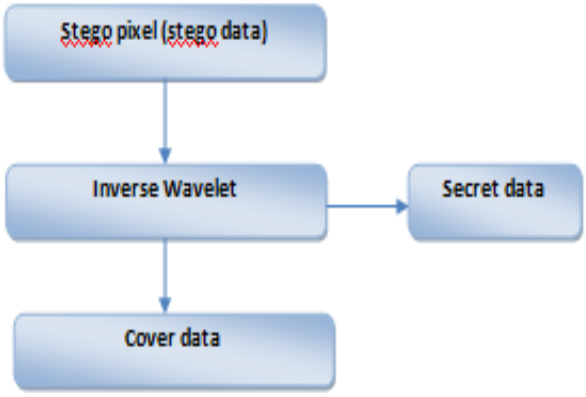

Fig.2. Extracting Flow chart

Module Description

In this method, four bits can be embedded with a maximum alternation of two bits. For further manipulation, we design the convolution decoder (4, 1) as shown in the Fig.3. This decoder circuit helps to change the amount of cover pixel in the image to produce a new stego image.

In the decoder circuit, the first five least significant bit planes of a pixel are given as inputs. The circuit performs the XOR operation and produces the outputs N1, N2, N3, and N4. Let the hidden message be a four bit message. If N1, N2, N3,N4 are the same as hidden message, there is no need to modify the cover image; if not, we should change the cover image in a way which causes the output of the decoder to be equal to the hidden message.

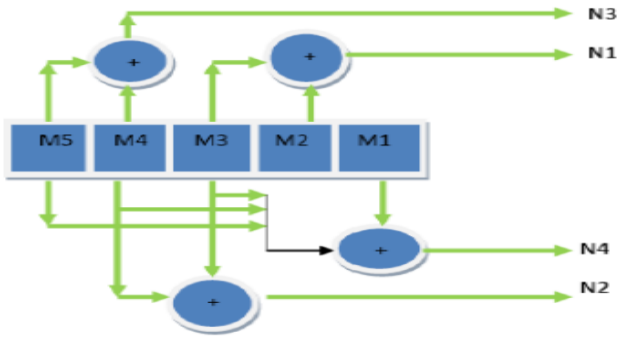

Fig.3. Cover to Stego object conversion Circuit

The procedure for how each pixel of the cover image must change according to different messages is shown in the Table. In all the cases, by changing only one or two gray levels of cover image, the secret data can be embedded in the pixel. The difference between method 1 and this method is that the embedding capacity is increased compared to method 1. It can be seen that in most cases by changing only one or two gray levels of cover image, the secret

ISSN: 2277-9655
Impact Factor: 1.852

data can be embedded in the cover pixel resulting in a new stego image.

Pixel	Decoder output	Message bits coming out of decoder	How cover change should change in order to result in the desired message	Changes in gray level of cover pixel
			Message	Gray-level change
00000000	0000	0000	0001	1
			0010	1,5
			0011	5
			0100	4,5
			0101	2,3
			0110	1,4
			0111	4
			1000	2
			1001	1,2
			1010	3,4
			1011	2,5
			1100	1,3
			1101	3
			1110	3,5
			1111	2,4
00000001	0001	0001	0000	1
			0010	5
			0011	1,4
			0100	1,5
			0101	4,5
			0110	4
			0111	1,3
			1000	1,2
			1001	2
			1010	2,4
			1011	2,5
			1100	3
			1101	1,3
			1110	2,3
			1111	3,4

Procedure for changing the 4 least significant bits of a pixel according to three bit Messages

Above table shows how the four bit information is embedded in the pixel. Let us consider an example where (say) the pixel of a cover image be taken as 01101010.Consider the five least significant bits of the pixel 01010. This is given as input to the decoder. The output of the decoder will be 0001.Suppose the data which is going to be embedded in the pixel is 0001, it will result in the stego pixel value 01101010. If the data which is going to be embedded in the pixel is 0000, it would change the cover pixel in order to make the output of the decoder to be equal to the hidden information. Based on the manipulation, the cover pixel is changed as 01101011.

Algorithm for Embedding

Inputs: Secret data, Cover data
Output: Stego image with secret data embedded in it.
Step 1: Read the cover data.
Step 2: The five least significant bits of the pixel are given as inputs to the Decoder circuit.
Step 3: Read the secret data.
Step 4: Embed the secret data in the following manner.
a) By altering one bit of cover pixel. OR
b) By altering two bits of cover pixel (i.e. combination of any two bits).
c) If all the secret data has been embedded, then Go to step 5.
Step 5: Store the resulting image as stego data.
Step 6: Transmit the stego data.

Algorithm for Extraction

Step 1: Read the Stego data.
Step 2: Apply the five least significant bits of the pixel to the decoder circuit
Step 3: Extract the data from decoder output.
Step 4: If all data has been recovered, go to Step 5.
Step 5: store the resulting data as the secret data.

Error Metrics

The two main parameters used to calculate the quality of stego data are mean square error and peak signal to noise ratio.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{i,j} - Y_{i,j}\right)^2$$

Where, X i,j is Stego value and Y i,j is the cover object. The PSNR is calculated using the equation

$$PSNR = 10\log_{10}\left(\frac{I_{\max}^2}{MSE}\right)dB$$

Where Image is the intensity value of each pixel which is equal to 255 for 8 bit gray scale images. Higher the value of PSNR better the image quality

Input Design

The input is given in to the embedding phase in the form of a notepad file which would be already created in the folder were all matlab files are saved. The embedding module should be capable of with helding the secret data in the notepad file. It should be done using any lossless transform so that there will be no loss of data during the transformation part. They are mainly used to achieve the highest possible level of accuracy and also ensure that the input is acceptable and understood by the user.

Output Design

Output design plays a vital role in our project implementation as the original message should be retrieved at the output side. It should be designed in such a way that user should be able to understand it easily. Compared to existing systems the performance

of our proposed algorithm should be better i.e. it should be robust, the capacity of message that could be hided in the image should be more and no one should be able to find any difference in the stego image and the original image

Hardware Description

To implement our algorithm in real word we use FPGA Spartan Edk3 kit so that the transmission of the stego image is possible and the secrecy of the image remains compact to the user only. For implementing this hardware we use Xilinx 10.1 software so that we can transfer the programmings to the kit and we would be able to execute it. Here we use hyper terminals to see retrieved message and visual basic dialog box to retrieve the image out reading the pixel values.

References

[1] *Himanshugupta, Riteshkumar and Dr. SoniChanglani, "Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method", International Journal of Emerging Technology and Advanced Engineering, vol 3,Issue 6, June 2013.*

[2] *Dr. AhlamFadhilMahmood, Nada Abdul Kanal and Sana sami Mohmmed, "An FPGA Implementation of secured Steganography Communication system", Tikrit Journal of Engineering Sciences, vol.19 No.4 December 2012,(14-23)*

[3] *S.A.Khandekar and Mrs. MR. Dixit, " Steganography for Text Messages Using Image" , IOSR Journal of Electronics and Communication Engineering, ISSN: 2278-2834 Volume 2, Issue 3(July-Aug 2012), PP 01-04*

[4] *Vijay Kumar Sharma and Vishal Shrivastava, " A Steganography algorithm for Hiding Data in Image by Improved LSB Substitution by Minimize Detection", Journal of Theoretical and Applied Information Technology, 15th February 2012, Vol36 No.1*

[5] *H.B.Kekre, A.A. Athawale , S.A. Patki ," Improved Steganalysis of LSB Embedded Color Images based on Stego-Sensitive Threshold Close Color Pair Signature", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 2 Feb 2011, PP. 836-842.*

[6] *B. Xia, X. Sun, J. Qin," Steganalysis Based on Neighbourhood Node Degree Histogram for LSB Matching Steganography", International Conference on Multimedia Information Networking and Security, IEEE Computer Society Washington, USA ,18-20 November , 2009, PP.79-82.*

[7] *C.Lin, C. Chang, W. Lee, and J. Lin," A Novel Secure Data Hiding Scheme Using a Secret Reference Matrix", Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kyoto, Japan, 12-14 September 2009.*

[8] *Hardik Patel, Preeti Dave / International Journal of Engineering Research and Applications(IJERA) ISSN: 2248-9622 www.ijera.comvol. 2, Issue 1,Jan-Feb 2012, pp.713-717*

[9] *On The Limits of Steganography Ross J. Anderson, Fabien A.P. Petitcolas IEEE Journal of Selected Areas in Communications,16(4):474-481, May 1998.Special Issue on Copyright & Privacy Protection. ISSN 0733-8716.*

[10] *A Steganography Implementation based on LSB & DCT Gurmeet Kaur* and Aarti Kochhar. Department of Electronics and Communication Engineering, CEM Kapurthala. Department of Electronics and Communication Engineering, DAVIET Jalandhar(Received 05 November 2012 Accepted 16 November 2012)*

[11] *A DWT Based Approach for Image Steganography Po-Yueh Chen* and Hung-Ju Lin Department of Computer Science and Information Engineering, National Changhua University of Education,No. 2 Shi-Da Road, Changhua City 500, Taiwan, R.O.C.*